EX PARTE OR LATE FILED

DOCKET FILE COPY ORIGINAL

mts INCORPORATED
TOWER RECORDS • BOOKS • VIDEO
2500 DEL MONTE, P.O. BOX 919001, WEST SACRAMENTO, CALIFORNIA 95691 (916) 373-2500

CC Docket No. 93-292

February 2, 1994

RECEIVED
FEB 25 1994
FCC - MAIL ROOM

Mr. William F. Canon
Acting Secretary
Federal Communications Commission
Common Carrier Bureau
1919 M St. N.W.
Washington D.C. 20554

Dear Mr. Canon,
Concerning the F.C.C.'s current position of proposing new rules regarding "Toll Fraud", I would like to voice a few comments on my company's behalf. Please take a moment to consider these comments as described below.

First I appreciate and applaud the Commission's position in trying to protect the user's interest. Even though I believe that all parties should be involved in the thwarting of this crime, currently the end user is the one taking all the brunt.

The topic of requiring PBX manufacturers to notify their customers of the risk of abuse to their equipment seems perfectly logical to me. ATT is doing this now. As I mentioned above this crime is everyone's problem and everyone should address it. But how can a user take any action if the're not aware of it. I've noticed that even with all of the media coverage about this topic lately, very few people are aware of exactly what is happening, and how.

Education benefits all parties, including the manufacturer. As an example; perhaps a manufacturer could brag that, because of their excellent toll fraud education program, they have the lowest rate of fraud of any PBX. Or perhaps PBX manufacturers could offer a "Toll Fraud Option Package" that helps detect fraud. Another suggestion is that PBX manufacturers don't put in default passwords. Every Master padlock comes with a unique combination; why can't a phone system.

I also agree that carriers should notify their customers as well, perhaps by the way of a bill insert. But please, let's not get carried away with so many regulations that they are spending there resources stuffing envelopes and complying with rules instead of addressing the problem, or truly educating PBX customers. I don't feel it's necessary that residential customers fully understand the possible problems that a PBX user with an 800 number is likely to encounter.

No. of Copies rec'd 0+2
List A B C D E

mts
INCORPORATED
TOWER RECORDS • BOOKS • VIDEO
2500 DEL MONTE, P.O. BOX 919001, WEST SACRAMENTO, CALIFORNIA 95691 (916) 373-2500

I do believe long distance carriers have an obligation to participate in this process of education and prevention. Reasons being, that they are a public utility. One reason they are allowed to exist is to benefit the public. They do need to be involved in this fight against Toll Fraud.

I don't feel however that carriers should be held fully responsible for the liability of a Toll Fraud problem any more than a electric company should be held responsible if an unauthorized person uses electricity. But, due to the large risks that are involved, and due to the fact that the technology exists for some type of monitoring, and that I can't lock up my phone numbers like I can turn off electricity, I would like to see some type of joint responsibility. Most of the carriers have the technology to notify a customer of a potential problem (This is especially critical for "calling cards"). And I believe they should be obliged to do so. On the other hand customers should take steps to protect themselves as well. For example I use a software package called Microtel. I have not been "hit" yet (to my knowledge) but this program keeps an eye on all long distance calls going through our PBX.

Perhaps, apportioning costs could be regulated by some type of program. Where a security audit is made and if all parties agree that if a problem arises,cost would be split 50/50. For example, the carrier agrees to notify the customer if his 800 usage goes above one thousand dollars in a twenty-four hour period, and in return the user completes an audit that shows he has met all the criteria for protecting his equipment.

Regarding services such as MCI Detect and ATT NetPROTECT etc. I agree with the letter dated Jan. 13 1994 sent to you by the SDN Users Association. These are basically insurance policies. I don't believe they are effective in addressing the problem.

As far as remote access port protection is concerned, I do not have any first hand knowledge regarding these products. But I am investigating them now. Some of these are reviewed in the August 1993 issue of Teleconnect magazine.

I hope I have given you some ideas and some insight as to how my company feels regarding this problem. We are very concerned that this type of risk exists, and that we have no recourse in the event that something does happen. I do hope the F.C.C. is able to implement some regulations that not only protect us "little guys" but also work on solving (or at least deterring) the problem.

Sincerely Yours,

Martin Sockolov